UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,499	02/28/2002	Zhichen Xu	100200290-1	7480

22879 7590 07/21/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
07/21/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ZHICHEN XU and LI XIAO

Appeal 2008-006311
Application 10/084,499[1]
Technology Center 2400

Before HOWARD B. BLANKENSHIP, JEAN R. HOMERE, and JAMES R. HUGHES, *Administrative Patent Judges*.

HUGHES, *Administrative Patent Judge*.

DECISION ON APPEAL[2]

---

[1] Application filed February 28, 2002. The real party in interest is Hewlett-Packard Development Co., L.P. (App. Br. 3.)

[2] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

STATEMENT OF THE CASE

The Appellants appeal from the Examiner's rejection of claims 1, 3-12, 14-25, 27-30, and 42-44 under authority of 35 U.S.C. § 134(a). Claims 2, 13, 26, and 31-41 have been canceled. The Board of Patent Appeals and Interferences (BPAI) has jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

Appellants' Invention

Appellants invented a method of increasing peer privacy by selecting a number of peers and updating a table in each peer with path index information for a path from an information provider to an information requestor. The method comprises forming a path from the provider to the requestor by selecting a plurality of peers in response to receiving a request for information, updating a table on each selected peer with a respective path index entry for the path (of the information), transmitting a message – comprising the requested information and a path index for the path of the information – from the provider to the requestor through the peers, determining a next peer for the path of the information by searching the table of each peer using the path index, retrieving the identity of the next peer in the path from the table, forming and transmitting a message to the next peer comprising the information and the path index encrypted with a public key of the next peer. (Spec 2, ll. 9-17; 6, l. 3 to 7, l. 6.)[3]

---

[3] We refer to Appellants' Specification ("Spec."); Amended Appeal Brief ("App. Br.") filed June 13, 2007; and Reply Brief ("Reply Br.") filed November 1, 2007. We also refer to the Examiner's Answer ("Ans.") mailed October 5, 2007.

Representative Claims

Independent claims 1 and 42 further illustrate the invention. They read as follows:

1. A method for increasing privacy, comprising:

forming a path from a provider to a requestor by selecting a plurality of peers in response to receiving a request for information;

updating a table on each peer of said plurality of peers with a respective path index entry for said information;

transmitting a message to said requestor through said plurality of peers, said message comprising said information and a path index for said information from said provider;

determining a next peer according to said path for said information by searching said table of each peer of said plurality of peers with said path index as an index into said table;

retrieving an identity of said next peer according to said path for said information and a respective index peer of said next peer;

encrypting said path index with a public key of said respective index peer of said next peer to form a next state of said path index; and

transmitting a new message with said information and said next state of said path index as said path index to said next peer.

42. A method for increasing privacy, comprising:

forming a path for information from a provider to a requestor through a plurality of peers in response to a received request for said information;

transmitting to each peer of said plurality of peers a respective set-up message comprising of a predetermined label and an identity of a next peer for said information;

> if a label stored at an intermediate peer of the plurality of peers does not match the predetermined label in the set-up message, the intermediate peer stores the predetermined label and the corresponding identity of the next peer;
>
> if a label stored at the intermediate peer matches the predetermined label, the intermediate peer retrieves a previously stored message and generates a next state of the predetermined label for the setup message; and
>
> transferring said information over said path in a message by determining a next peer according to said path by matching a message label included in said message to said predetermined label.

References

The Examiner relies on the following reference as evidence of unpatentability:

David M. Goldschlag, Michael G Reed, & Paul F. Syverson, *Hiding Routing Information*, Proceedings of the First International Workshop on Information Hiding, 1-13 (1996) (hereinafter "Goldschlag").

Ian Clarke, Oskar Sandberg, Brandon Wiley, Theodore W. Hong, *Freene, A Distributed Anonymous Information Storage and Retrieval System*, Lecture Notes in Computer Science, 1-21(2000) (hereinafter "Clarke").

Rejection on Appeal

The Examiner rejects claims 42-44 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.[4]

[4] The Examiner has withdrawn a separate rejection of claim 44 under 35 U.S.C. § 112, first paragraph. (Ans. 19.)

The Examiner rejects claims 1, 8-12, 20-25, 27-30, and 42-44 under 35 U.S.C. § 102(b) as being anticipated by Goldschlag.

The Examiner rejects claims 3-7 and 14-19 under 35 U.S.C. § 103(a) as being unpatentable over the combination of Goldschlag and Clarke.

The Examiner also objects to the Appellants' Specification under 37 C.F.R. § 1.75(d) for failing to provide proper antecedent basis for the claimed subject matter.[5]

ISSUES

Based on our review of the administrative record, Appellants' contentions, and the Examiner's findings and conclusions, the pivotal issues before us are as follows.

1. Does the Examiner err in finding that Appellants' limitation reciting "if a label stored at an intermediate peer of the plurality of peers does not match the predetermined label in the set-up message" does not comply with the written description requirement under 35 U.S.C. § 112, first paragraph?

2. Does the Examiner err in finding the Goldschlag reference discloses a respective index peer of the next peer and encrypting the path index with a public key of the respective index peer?

---

[5] As pointed out by the Examiner (Ans. 2), the Examiner's objection to the Appellants' Specification under 37 C.F.R. § 1.75(d) is a petitionable matter, rather than an appealable matter. We must carefully observe the "line of demarcation between appealable matters for the Board of Patent Appeals and Interferences (Board) and petitionable matters for the Director of the U.S. Patent and Trademark Office (Director)." MPEP § 1201. Therefore, we do not address this issue as it is not properly brought before us.

3. Does the Examiner err in finding the Goldschlag reference discloses comparing a label stored in a peer to a predetermined label in a set-up message, storing the predetermined label and a corresponding identity of the next peer if there is no match, and retrieving a previously stored message to generate a next state of the predetermined label for the setup message if a match occurs?

FINDINGS OF FACT (FF)

Goldstein Reference

1. Goldschlag describes network architecture and corresponding messages for providing real-time, bi-directional, anonymous communication utilizing a proxy service. (p. 1, Abst. & sec. 1, para. 2; p. 2, para. 1; Fig. 1.) Goldschlag's messages ("onions") comprise layers "of encryption wrapped around a payload." (p. 4, sec. 3, para. 2.) The proxy for the initiator of the communication determines a route to a responder's (message recipient's) proxy through a number of routing nodes and sends an onion along the route to establish a virtual circuit. Utilizing the route information, the initiator's proxy first forms the innermost layer of the onion by encrypting the responder's proxy information and the payload. Then the initiator's proxy forms the additional layers by encrypting the information for each preceding node along the route back to initiator's proxy. (pp. 4-6, sec. 3; Fig. 2.)

2. The onion message contains "a circuit identifier, a command (*create, destroy, and data*), and data." (p. 6, sec. 3.1, para. 1.) The initiator sends the onion message along the route, where each node peels off and decrypts a respective layer of the onion, and also stores a copy of the onion. (pp. 4-7, sec. 3 & 3.1, Figs. 2 & 3.) The node also compares the received

onion to a table of onions (virtual circuit identifiers, cryptographic functions, and a keys) stored in the node. (pp. 5-6, sec. 3 & 3.1; p. 10, sec. 4, para. 4.) When a node along the route receives a create command along with an onion, the node: retrieves a virtual circuit identifier, a cryptographic function, and a key for the next node from a table in the node; applies the cryptographic function and key; and sends another create message containing this identifier and the onion to the next node in the route. (pp. 4-7, sec. 3 & 3.1; pp. 10-11, sec. 4; Figs. 2 & 3.)

3. The message forwarding the onion includes a header and a payload field. The header includes the virtual circuit identifier and command. The payload includes the onion. The payload of the message is encrypted using the public key of the next peer, but the header of the message is not encrypted with the public key of the next peer. (p. 10, sec. 4, para. 3.)

ANALYSIS

Issue 1: Rejection of Claims 42-44 under § 112, first paragraph

The Examiner finds that Appellants' claims 42-44 contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention. Specifically, the Examiner finds that Appellants' claim requires storing a received label in a table of a peer if any label stored within the table does not match the received label:

> whether or not the received label is found to exist as an entry within the hash table, the peer will store the received label upon the condition that *a label* stored within the hash table does not

> match the received label. In other words, as long as the hash table contains entries wherein one of the entries ("a label") does not match the received label, then the received will be stored.

(Ans. 4.) The Examiner finds that this is not the "true operation" of Appellants' invention, and instead, a determination is made whether the received label is found in the hash table. (Ans. 4.)

Appellants contend that the specification as originally filed "clearly discloses the features" of the claims. (App. Br. 18.) In particular, Appellants contend that:

> [T]he peer privacy module 220 at an intermediate peer may be configured to search the hash table 225 for an existing entry matching the received current label. If the existing entry is not present, the hash table 225 may be updated with the label and the corresponding identity for the next peer according to the path. Otherwise, if there is an existing entry, the peer privacy module 220 may be configured [to] determine the next peer according to the path and to retrieve a previously stored message.

(App. Br. 17-18.)

After reviewing the record on appeal, we find Appellants' arguments to be persuasive. We agree with Appellants' construction of the disputed claim limitation, and find the Examiner has misinterpreted the claim language. Appellants provide support for the disputed limitation in their Specification as originally filed. (App. Br. 17-18, citing Spec. 11-13, 15, 17, 25, 27 & Fig. 7A.) Accordingly, we find that a skilled artisan would understand the cited portions of the Specification to describe searching the hash table for an existing label entry matching the received current label, and storing the received current label if no match is found. "[T]he test for sufficiency is whether the disclosure of the application relied upon

reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date. *Ariad Pharmas. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (quoting *Vas-Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1562-63 (Fed. Cir. 1991) (citations omitted)). We agree with the Examiner that Appellants' claim language and Specification are not the model of clarity in this regard; however, we find that the Specification would reasonably convey possession of the claimed limitation to one skilled in the art as of the filing date.

For the foregoing reasons, Appellants have persuaded us of error in the Examiner's written description rejection of claims 42-44. Accordingly, we reverse the Examiner's written description rejection of these claims.

Issue 2: Rejection of Claims 1, 8-12, 20-25, and 27-30 under § 102

The Examiner finds that the Goldschlag reference discloses each feature of Appellants' claims, and provides a detailed explanation as to why Appellants' arguments fail to overcome the Examiner's anticipation rejection. (Ans. 5-12, 20-24.) Specifically, the Examiner finds that Goldschlag discloses index peers, as well as encrypting the path index with a public key of the respective index peer. (Ans. 20-22.) Appellants, on the other hand, contend that the Goldschlag reference does not disclose index peers, or encrypting the path index with the public key of the index peer of the next peer. (App. Br. 20; Reply Br. 6-7.) Accordingly, we decide the question of whether the Examiner erred in finding the Goldschlag reference discloses a respective index peer of the next peer and encrypting the path index with a public key of the respective index peer.

After reviewing the record on appeal, we find Appellants' arguments to be persuasive. We agree with Appellants that the Goldschlag reference does not disclose index peers, or encrypting the path index with the public key of the respective index peer.

Goldschlag discloses determining a route between an initiator and a responder through a number of routing nodes, and sending an onion along the route to establish a virtual circuit. The initiator utilizes the route to build the onion by encrypting the route and node information in layers, starting with the responder at the innermost layer, and adding (layering) encrypted information for each preceding node along the route back to the initiator. As the onion proceeds along the route, each node peels off and decrypts a respective layer of the onion, and stores a copy of the onion. From the peeled layer of information, the node determines a virtual circuit identifier for the next node in the route, as well as a cryptographic function and a key for the next node. The node sends the onion to the next node in the route, and encrypts data sent along the path with the cryptographic function and key from the onion. (FF 1-2.) The message forwarding the onion is encrypted using the public key of the next peer (FF 1-2), but the header of the message including the virtual circuit identifier is not encrypted with the public key of the next peer (FF 3).

The dispute before us hinges on whether Goldschlag discloses "index peers" as claimed. In particular, the Examiner and Appellants disagree on what constitutes an index peer, and the construction of this feature is critical to resolving this dispute. We begin our analysis by construing Appellants' claim, giving the claim the "broadest reasonable interpretation consistent with the [S]pecification" and "claim language should be read in light of the

[S]pecification as it would be interpreted by one of ordinary skill in the art." *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004) (citations omitted). The Examiner appears to construe an index peer simply as a peer including index information. (Ans. 20-21.) Accordingly, the Examiner finds that the peers in the path described by Goldschlag are index peers. (Ans. 20-22.) We disagree. Although Appellants do not explicitly define an index peer in their Specification, Appellants explain that index peers are "a second selected group of peers" (Spec. 20, ll. 18-19) distinct from the group of peers in the path between the provider and requestor. (Spec. 20, l. 9 to 21, l. 2.) Thus, we find that the recited "respective index peer of said next peer" – said next peer being the next peer in the path between the provider and requestor – cannot be the next peer in the path. Therefore, we find Goldschlag does not disclose index peers.

Assuming, *arguendo*, we were to agree with the Examiner that Goldschlag discloses index peers (which we do not), Goldschlag does not disclose encrypting the path index with a public key of the respective index peer of the next peer. Although Appellants do not explicitly define a "path index" in their Specification, Appellants explain that a path index "comprises an individual predetermined label and a corresponding next peer," where "the predetermined label [is] generated for each peer . . . to determine the next hop for the information according to the path," and the "peer [uses the] received label . . . as a search index into the hash table 225 to determine the next hop for the information." (Spec. 13, ll. 8-13.) Thus, we find that the recited "path index" is an identifier of the next hop or peer in the path. This is equivalent to Goldschlag's virtual circuit identifier. As we explain *supra*, Goldschlag does not encrypt the message header,

including the virtual circuit identifier, with a public key of any kind. And, Goldschlag uses a private encryption function and key to encrypt the layers of the onion. Thus, Goldschlag does not disclose encrypting the path index with a public key of the respective index peer of the next peer.

We therefore find that Goldschlag does not disclose each feature of Appellants' claim 1. Appellants' independent claims 12 and 21 include limitations of commensurate scope. Thus, Appellants persuade us of error in the Examiner's anticipation rejection of claims 1, 8-12, 20-25, and 27-30. And, accordingly, we must reverse the Examiner's anticipation rejection of Appellants' claims 1, 8-12, 20-25, and 27-30.

Issue 2: Rejection of Claims 42-44 under § 102

Appellants' independent claim 42 differs in scope from the claims discussed *supra*, and does not include limitations directed to index peers or encrypting a path index. Rather, claim 42 is directed to comparing and manipulating label information. The Examiner finds that the Goldschlag reference discloses each feature of Appellants' claim 42, and provides a detailed explanation as to why Appellants' arguments fail to overcome the Examiner's anticipation rejection. (Ans. 11-12, 23-24.) Specifically, the Examiner finds that Goldschlag discloses comparing and storing messages including the identity of the next peer, as well as formatting and forwarding messages to a next peer in a path. (Ans. 11-12.) Appellants, contend that "[t]here is no comparison performed in Goldschlag to determine whether there is a match or is not a match between a label in a received set-up message and a stored label." (App. Br. 26.) Appellants also contend that Goldschlag doesn't disclose "generating a next state of the predetermined

label," and "storing the predetermined label and the corresponding identity of the next peer," depending on whether there is a match. (App. Br. 26.) Accordingly, we decide the question of whether the Examiner erred in finding the Goldschlag reference discloses comparing a label stored in a peer to a predetermined label in a set-up message, storing the predetermined label and a corresponding identity of the next peer if there is no match, and retrieving a previously stored message to generate a next state of the predetermined label for the setup message if a match occurs.

After reviewing the record on appeal, we agree with the Examiner (and find that) the Goldschlag reference discloses the disputed features. Specifically, we find that the recited label (and predetermined label) is equivalent to the previously discussed "path index," which is an identifier of the next hop or peer in the path. As explained *supra*, this is equivalent to Goldschlag's virtual circuit identifier. As we also explained *supra*, Goldschlag sends the onion along a route between the initiator and responder, each node peels off and decrypts a respective layer of the onion, and each node stores a copy of the onion. In particular, we find that Goldschlag discloses a node comparing the received onion to a table of onions stored in the node, and retrieving a virtual circuit identifier for the next node from a table in the node. (FF 2.) Thus, we find Goldschlag discloses receiving an identifier (label) in an onion (set-up message), storing the onion and identifier, comparing the stored onion and identifier to received onions and identifiers, and retrieving a stored onion and identifier to "create" (generate) an onion and identifier for the next virtual circuit. We therefore are not persuaded of error in Examiner's anticipation rejection of claim 42.

Appellants' dependent claim 43 includes a limitation of "encrypting the received predetermined label with a public key of a respective index peer of the next peer." (App. Br. 27.) We find, for the same reasons discussed with respect to claim 1 (*supra*), that Goldschlag does not disclose encrypting the a next peer identifier (label) with a public key of the respective index peer of the next peer. We therefore find that Goldschlag does not disclose each feature of Appellants' claim 43, and accordingly, we must reverse the Examiner's anticipation rejection of this claim.

Appellants' do not separately argue dependent claim 44. Nor, do they otherwise address the recited limitation of "an encryption key encrypted with the public key of the requestor." (App. Br. 41, Claim App'x, claim 41; *see also* claim 21.) Appellants do not present arguments with respect to this limitation in their discussion of claim 21 (App. Br. 25). Therefore, we select independent claim 42 as representative of this claim. Consequently, Appellants have not persuaded us to find error in the Examiner's anticipation rejection of dependent claim 44, for the reasons set forth in our discussion of independent claim 42 (*supra*). *See* 37 C.F.R. § 41.37(c)(1)(vii) (2007). Thus, we affirm the Examiner's anticipation rejection of Appellants' claims 42 and 44.

Rejection of Claims 3-7 and 14-19 under § 103

Appellants' dependent claims 3-7 and 14-19 depend from independent claims 1 and 12, respectively. By virtue of their dependence on these base claims, claims 3-7 and 14-19 recite the limitations of dependent claim 1 discussed *supra*. Accordingly, we find Goldschlag fails to disclose, teach, or suggest all the features of these claims, and Clarke does not cure these

deficiencies. Therefore, Appellants have persuaded us of error in the Examiner's obviousness rejection of claims 3-7 and 14-19 for the reasons set forth *supra*. Accordingly, we must reverse the Examiner's obviousness rejection of these claims.

CONCLUSIONS OF LAW

The Examiner did not err in finding the Goldschlag reference discloses comparing a label stored in a peer to a predetermined label in a set-up message, storing the predetermined label and a corresponding identity of the next peer if there is no match, and retrieving a previously stored message to generate a next state of the predetermined label for the setup message if a match occurs.

The Examiner, however, erred in finding that: (1) Appellants' limitation reciting "if a label stored at an intermediate peer of the plurality of peers does not match the predetermined label in the set-up message" does not comply with the written description requirement under 35 U.S.C. § 112, first paragraph; and (2) the Goldschlag reference discloses a respective index peer of the next peer and encrypting the path index with a public key of the respective index peer.

DECISION

We affirm the Examiner's rejection of claims 42 and 44 under 35 U.S.C. § 102(b).

We reverse the Examiner's rejections of claims 42-44 under 35 U.S.C. § 112, first paragraph.

We reverse the Examiner's rejections of claims 1, 8-12, 20-25, 27-30, and 43 under 35 U.S.C. § 102(b).

We reverse the Examiner's rejections of claims 3-7 and 14-19 under 35 U.S.C. § 103(a).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

erc

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS CO 80528